



CVE-2023-20849

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-20849
State	PUBLIC
Assigner	security@mediatek.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-04 03:15:00 UTC
Updated	2023-09-07 14:44:00 UTC
Description	In imgsys_cmdq, there is a possible use after free due to a missing valid range checking. This could lead to local escalation

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	11.0	All	All	All
Operating System	Google	Android	12.0	All	All	All
Operating System	Linux	Linux Kernel	6.1	-	All	All
Application	Linuxfoundation	Yocto	4.0	All	All	All
Application	Mediatek	lot Yocto	23.0	All	All	All
Hardware	Mediatek	Mt2713	-	All	All	All
Hardware	Mediatek	Mt6895	-	All	All	All
Hardware	Mediatek	Mt6897	-	All	All	All
Hardware	Mediatek	Mt6983	-	All	All	All
Hardware	Mediatek	Mt8188	-	All	All	All
Hardware	Mediatek	Mt8195	-	All	All	All
Hardware	Mediatek	Mt8395	-	All	All	All
Hardware	Mediatek	Mt8781	-	All	All	All

References

Reference	Source	Link	Tags
September 2023	MISC	corp.mediatek.com	

CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis
No vendor comments have been submitted for this CVE.			
There are currently no legacy QID mappings associated with this CVE.			

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report